

SECS1024 - Laboratoire 3 - API REST

Authentification

Ce laboratoire est noté - 10 points - 10% de la note finale

Objectif : utiliser l'API REST de wordpress pour l'authentification des utilisateurs

Mikael Lacroix

1 Installation de Wordpress

Sous VirtualBox, sur le réseau interne, installez et configurez Wordpress sur un serveur Linux pour qu'il affiche une page web d'accueil (<https://ubuntu.com/tutorials/install-and-configure-wordpress>)

2 API REST

Pour cette partie, vous allez utiliser la commande curl pour interagir avec l'API REST de wordpress. Vous devez illustrer vos réponses avec une capture écran de la commande et de la réponse obtenue. Voici les options utiles de la commande curl :

`curl -X [opération] -i http://wordpress.local/wp-json/wp/v2/ressources -d [data]`

Créez une commande curl qui permet de recevoir la liste de tous les utilisateurs de votre site wordpress ? (1 point)

```
(kali@kali2024blue)-[~]
$ curl -X GET -i http://10.0.67.244/wp-json/wp/v2/users
HTTP/1.1 200 OK
Date: Thu, 30 Jan 2025 17:53:40 GMT
Server: Apache/2.4.58 (Ubuntu)
X-Robots-Tag: noindex
Link: <http://10.0.67.244/wp-json/>; rel="https://api.w.org/"
X-Content-Type-Options: nosniff
Access-Control-Expose-Headers: X-WP-Total, X-WP-TotalPages, Link
Access-Control-Allow-Headers: Authorization, X-WP-Nonce, Content-Disposition, Content-MD5, Content-Type
X-WP-Total: 2
X-WP-TotalPages: 1
Allow: GET
Vary: Origin
Content-Length: 1243
Content-Type: application/json; charset=UTF-8

[{"id":2,"name":"Jean-Marc Solution","url":"","description":"","link":"http://10.0.67.244/author/jean-marc/","slug":"jean-marc","avatar_urls":{"24":"https://secure.gravatar.com/avatar/09c9f88de7f4b5f1665c4bffb8eac9fc?s=24&d=mm&r=g","48":"https://secure.gravatar.com/avatar/09c9f88de7f4b5f1665c4bffb8eac9fc?s=48&d=mm&r=g","96":"https://secure.gravatar.com/avatar/09c9f88de7f4b5f1665c4bffb8eac9fc?s=96&d=mm&r=g"},"meta":{"_links":{"self":{"href":"http://10.0.67.244/wp-json/wp/v2/users/2"},"collection":{"href":"http://10.0.67.244/wp-json/wp/v2/users/"}}},"id":1,"name":"Ubuntu","url":"http://10.0.67.244","description":"","link":"http://10.0.67.244/author/ubuntu/","slug":"ubuntu","avatar_urls":{"24":"https://secure.gravatar.com/avatar/2672049e12d6caf8633f13a917b22fae?s=24&d=mm&r=g","48":"https://secure.gravatar.com/avatar/2672049e12d6caf8633f13a917b22fae?s=48&d=mm&r=g","96":"https://secure.gravatar.com/avatar/2672049e12d6caf8633f13a917b22fae?s=96&d=mm&r=g"},"meta":{"_links":{"self":{"href":"http://10.0.67.244/wp-json/wp/v2/users/1"},"collection":{"href":"http://10.0.67.244/wp-json/wp/v2/users/"}}},"targetHints":{"allow":["GET"]}}],"collection":{"href":"http://10.0.67.244/wp-json/wp/v2/users/"}}]

(kali@kali2024blue)-[~]
```

Créez une commande curl qui permet de recevoir la liste de tous les posts de votre site wordpress ? (1 point)

```
(kali@kali2024blue)-[~]
$ curl -X GET -i http://10.0.67.244/wp-json/wp/v2/posts
HTTP/1.1 200 OK
Date: Thu, 30 Jan 2025 17:57:40 GMT
Server: Apache/2.4.58 (Ubuntu)
X-Robots-Tag: noindex
Link: <http://10.0.67.244/wp-json/>; rel="https://api.w.org/"
X-Content-Type-Options: nosniff
Access-Control-Expose-Headers: X-WP-Total, X-WP-TotalPages, Link
Access-Control-Allow-Headers: Authorization, X-WP-Nonce, Content-Disposition, Content-MD5, Content-Type
X-WP-Total: 2
X-WP-TotalPages: 1
Allow: GET
Vary: Origin
Content-Length: 3666
Content-Type: application/json; charset=UTF-8

[{"id":8,"date":"2025-01-30T17:53:14","date_gmt":"2025-01-30T17:53:14","guid":{"rendered":"http://10.0.67.244/?p=8"},"modified":"2025-01-30T17:53:14","modified_gmt":"2025-01-30T17:53:14","slug":"pierre-jean-pour-vous-aider","status":"publish","type":"post","link":"http://10.0.67.244/2025/01/30/pierre-jean-pour-vous-aider/","title":{"rendered":"Pierre-jean pour vous aider"},"content":{"rendered":"\u003csalut les amis\u003c\/p\u003e\u003cp\u003esalut les amis\u003c\/p\u003e","protected":false,"excerpt":{"rendered":"\u003cp\u003esalut les amis\u003c\/p\u003e","protected":false},"author":2,"featured_media":0,"comment_status":"open","ping_status":"open","sticky":false,"template":"","format":"standard","meta":{"footnotes":"","categories":[1],"tags":[],"class_list":["post-8","post","type-post","status-publish","format-standard","hentry","category-uncategorized"],"links":{"self":{"href":"http://10.0.67.244/wp-json/wp/v2/posts/8"},"targetHints":{"allow":{"GET"}}},"collection":{"href":"http://10.0.67.244/wp-json/wp/v2/posts"},"about":{"href":"http://10.0.67.244/wp-json/wp/v2/types/post"},"author":{"embeddable":true,"href":"http://10.0.67.244/wp-json/wp/v2/users/2"},"replies":{"href":"http://10.0.67.244/wp-json/wp/v2/comments?post=8"},"version-history":{"count":2,"href":"http://10.0.67.244/wp-json/wp/v2/posts/8/revisions"},"predecessor-version":{"id":11,"href":"http://10.0.67.244/wp-json/wp/v2/posts/8/revisions/11"},"wp:attachment":{"href":"http://10.0.67.244/wp-json/wp/v2/media?parent=8"},"wp:term":{"taxonomy":"category","embeddable":true,"href":"http://10.0.67.244/wp-json/wp/v2/categories?post=8"},"taxonom":{"taxonomy":"post_tag","embeddable":true,"href":"http://10.0.67.244/wp-json/wp/v2/tags?post=8"},"curies":{"name":"wp","href":"https://api.w.org/{rel}"},"templated":true}}]}

(kali@kali2024blue)-[~]
$
```

Créez une commande curl qui permet de recevoir la liste du premier post de votre site wordpress ? Quel est son id ? (1 point)

```
(kali@kali2024blue)-[~]
$ curl -X GET -i http://10.0.67.244/wp-json/wp/v2/posts/1
HTTP/1.1 200 OK
Date: Thu, 30 Jan 2025 17:58:50 GMT
Server: Apache/2.4.58 (Ubuntu)
X-Robots-Tag: noindex
Link: <http://10.0.67.244/2025/01/23/hello-world/>; rel="alternate"; type=text/html
X-Content-Type-Options: nosniff
Access-Control-Expose-Headers: X-WP-Total, X-WP-TotalPages, Link
Access-Control-Allow-Headers: Authorization, X-WP-Nonce, Content-Disposition, Content-MD5, Content-Type
Allow: GET
Vary: Origin
Content-Length: 1826
Content-Type: application/json; charset=UTF-8

{"id":1,"date":"2025-01-23T17:34:16","date_gmt":"2025-01-23T17:34:16","guid":{"rendered":"http://10.0.67.244/?p=1"},"modified":"2025-01-23T17:34:16","modified_gmt":"2025-01-23T17:34:16","slug":"hello-world","status":"publish","type":"post","link":"http://10.0.67.244/2025/01/23/hello-world/","title":{"rendered":"Hello world!"},"content":{"rendered":"\u003cWelcome to WordPress. This is your first post. Edit or delete it, then start writing!\u003c\/p\u003e","protected":false},"excerpt":{"rendered":"\u003cWelcome to WordPress. This is your first post. Edit or delete it, then start writing!\u003c\/p\u003e","protected":false},"author":1,"featured_media":0,"comment_status":"open","ping_status":"open","sticky":false,"template":"","format":"standard","meta":{"footnotes":"","categories":[1],"tags":[],"class_list":["post-1","post","type-post","status-publish","format-standard","hentry","category-uncategorized"],"links":{"self":{"href":"http://10.0.67.244/wp-json/wp/v2/posts/1"},"targetHints":{"allow":{"GET"}}},"collection":{"href":"http://10.0.67.244/wp-json/wp/v2/posts"},"about":{"href":"http://10.0.67.244/wp-json/wp/v2/types/post"},"author":{"embeddable":true,"href":"http://10.0.67.244/wp-json/wp/v2/users/1"},"replies":{"href":"http://10.0.67.244/wp-json/wp/v2/comments?post=1"},"version-history":{"count":0,"href":"http://10.0.67.244/wp-json/wp/v2/posts/1/revisions"},"wp:attachment":{"href":"http://10.0.67.244/wp-json/wp/v2/media?parent=1"},"wp:term":{"taxonomy":"category","embeddable":true,"href":"http://10.0.67.244/wp-json/wp/v2/categories?post=1"},"taxonom":{"taxonomy":"post_tag","embeddable":true,"href":"http://10.0.67.244/wp-json/wp/v2/tags?post=1"},"curies":{"name":"wp","href":"https://api.w.org/{rel}"},"templated":true}}]}

(kali@kali2024blue)-[~]
$
```

3 Authentification basique API

Pour certaines opérations sur les ressources de wordpress, l'utilisateur doit être authentifié pour autoriser l'opération.

Sur wordpress, installez et activez le plugin "JSON Basic Authentification".

Vous devez illustrer vos réponses avec une capture écran de la commande et de la réponse obtenue.



WordPress REST API Authentication

By [miniOrange](#)

[Download](#)[Details](#)[Reviews](#)[Installation](#)[Development](#)[Support](#)

Add Plugins [Upload Plugin](#)

If you have a plugin in a .zip format, you may install or update it by uploading it here.

[Browse...](#) wp-rest-api-authentication.3.6.2.zip [Install Now](#)

miniOrange

Postman-Samples

Configuration Tracker

- Configure Authentication Method
- Basic Authentication Method Configurations (Pre-Configured)
- Save Configuration and Get Started

Configure Methods > Basic Authentication Method

[Back](#) [Next](#)

WordPress REST API - Basic Authentication Method involves the REST APIs access on validation against the API token generated based on the user's username, password and on basis of client credentials.


[Video Guide](#) [Setup Guide](#) [Developer Doc](#)

Select One of the below Basic Token generation types

- | | |
|--|---|
|
Username & Password with Base64 Encoding |
Username & Password with HMAC Validation Premium |
|
Client ID & Secret with Base64 Encoding Premium |
Client ID & Secret with HMAC Validation Premium |

Token Encryption Type Type: **Base 64 Encoding**

Test Configuration

ubuntu password 

REST API Endpoint:

GET http://10.0.67.244/wp-json/wp/v2/posts

Test Configuration

Note: The Test has been done successfully. Please click on "Finish" button on the top right corner of the screen to save the authentication method.

Request Headers


Authorization Basic dWJ1bnR1OnBhc3N3b3Jk

Response

```
[
  {
    "id": 8,
    "date": "2025-01-30T17:53:14",
    "date_gmt": "2025-01-30T17:53:14",
    "guid": {
      "rendered": "http://10.0.67.244/?p=8"
```

Token Encryption Type Type: **Base 64 Encoding**

Test Configuration

ubuntu dfedsfdf 

REST API Endpoint:

GET http://10.0.67.244/wp-json/wp/v2/posts

Test Configuration

Note: You are currently in the testing mode and this authentication method is not yet enabled on your site. Please click on "Finish" button on the top right corner of the screen to save the authentication method.

Request Headers

Authorization Basic dWJ1bnR1OmRmZWZmZmRm

Response

```
{
  "status": "error",
  "error": "INVALID_PASSWORD",
  "code": "400",
  "error_description": "Incorrect password."
}
```

Créez une commande curl qui permet de modifier le titre du premier post de votre site wordpress ? (1 point)


```
(kali@kali2024blue)-[~]
$ curl -X POST -i http://10.0.67.244/wp-json/wp/v2/posts/ -d '{"title":"michel"}' --user ubuntu:password -H "Content-Type:application/json"
HTTP/1.1 201 Created
Date: Tue, 04 Feb 2025 13:43:48 GMT
Server: Apache/2.4.58 (Ubuntu)
X-Robots-Tag: noindex
Link: <http://10.0.67.244/wp-json/>; rel="https://api.w.org/"
X-Content-Type-Options: nosniff
Access-Control-Expose-Headers: X-WP-Total, X-WP-TotalPages, Link
Access-Control-Allow-Headers: Authorization, X-WP-Nonce, Content-Disposition, Content-MD5, Content-Type
Location: http://10.0.67.244/wp-json/wp/v2/posts/15
Allow: GET, POST
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0, no-store, private
Content-Length: 2526
Content-Type: application/json; charset=UTF-8

{"id":15,"date":"2025-02-04T13:43:48","date_gmt":"2025-02-04T13:43:48","guid":{"rendered":"http://10.0.67.244/?p=15"},"raw":"http://10.0.67.244/?p=15"},"modified":"2025-02-04T13:43:48","modified_gmt":"2025-02-04T13:43:48","password":"","slug":"","status":"draft","type":"post","link":"http://10.0.67.244/?p=15","title":{"raw":"michel","rendered":"michel"},"content":{"raw":"","rendered":"","protected":false,"block_version":0},"excerpt":{"raw":"","rendered":"","protected":false},"author":1,"featured_media":0,"comment_status":"open","ping_status":"open","sticky":false,"template":"","format":"standard","meta":{"footnotes":"","categories":[1],"tags":[],"permalink_template":"http://10.0.67.244/2025/02/04/%postname%/","generated_slug":"michel","class_list":["post-15","post","type-post","status-draft"],"format-standard","hentry","category-uncategorized"},"_links":{"self":{"href":"http://10.0.67.244/wp-json/wp/v2/posts/15"},"targetHints":{"allow":["GET","POST","PUT","PATCH","DELETE"]},"collection":{"href":"http://10.0.67.244/wp-json/wp/v2/posts"},"about":{"href":"http://10.0.67.244/wp-json/wp/v2/types/post"},"author":{"embeddable":true,"href":"http://10.0.67.244/wp-json/wp/v2/users/1"},"replies":{"embeddable":true,"href":"http://10.0.67.244/wp-json/wp/v2/comments?post=15"},"version-history":{"count":0,"href":"http://10.0.67.244/wp-json/wp/v2/posts/15/revisions"},"wp:attachment":{"href":"http://10.0.67.244/wp-json/wp/v2/media?parent=15"},"wp:term":{"taxonomy":"category","embeddable":true,"href":"http://10.0.67.244/wp-json/wp/v2/categories?post=15"},"taxonomies":{"post_tag","embeddable":true,"href":"http://10.0.67.244/wp-json/wp/v2/tags?post=15"},"wp:action-publish":{"href":"http://10.0.67.244/wp-json/wp/v2/posts/15"},"wp:action-unfiltered-html":{"href":"http://10.0.67.244/wp-json/wp/v2/posts/15"},"wp:action-sticky":{"href":"http://10.0.67.244/wp-json/wp/v2/posts/15"},"wp:action-assign-author":{"href":"http://10.0.67.244/wp-json/wp/v2/posts/15"},"wp:action-create-categories":{"href":"http://10.0.67.244/wp-json/wp/v2/posts/15"},"wp:action-assign-categories":{"href":"http://10.0.67.244/wp-json/wp/v2/posts/15"},"wp:action-create-tags":{"href":"http://10.0.67.244/wp-json/wp/v2/posts/15"},"wp:action-assign-tags":{"href":"http://10.0.67.244/wp-json/wp/v2/posts/15"},"curies":{"name":"wp","href":"https://api.w.org/{rel}","templated":true}}}
```

Posts

Add New Post

All (3) | Mine (2) | Published (2) | Draft (1)

Search Posts

Bulk actions

Apply

All dates

All Categories

Filter

3 items

<input type="checkbox"/>	Title	Author	Categories	Tags		Date
<input type="checkbox"/>	michel — Draft	Ubuntu	Uncategorized	—	—	Last Modified 2025/02/04 at 1:43 pm
<input type="checkbox"/>	Pierre-jean pour vous aider	Jean-Marc Solution	Uncategorized	—	—	Published 2025/01/30 at 5:53 pm
<input type="checkbox"/>	piere-jean	Ubuntu	Uncategorized	—	1	Published 2025/01/23 at 5:34 pm
<input type="checkbox"/>	Title	Author	Categories	Tags		Date

Bulk actions

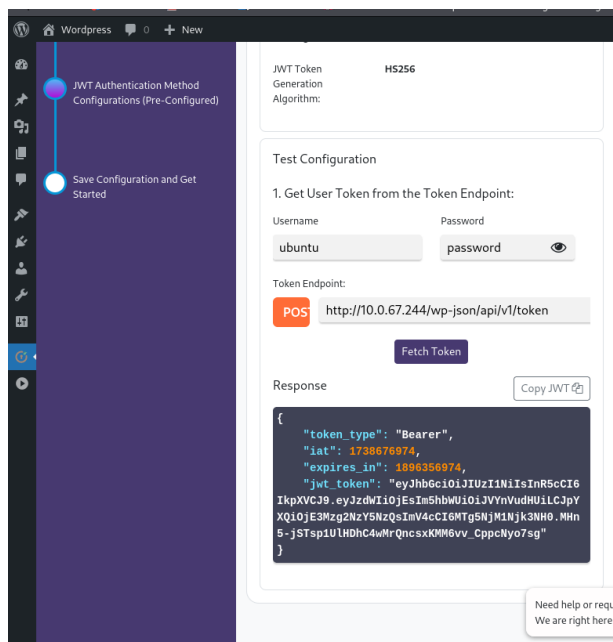
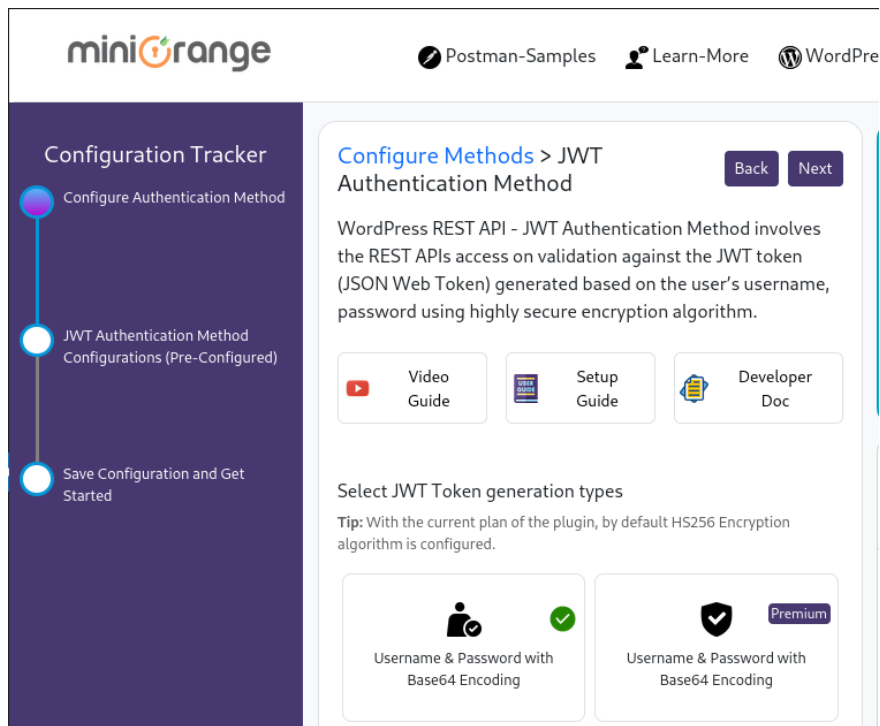
Apply

3 items

4 Authentication JWT API

Sur wordpress, installez et activez un plugin permettant une authentification des utilisateurs par un JWT.

Quel est ce plugin ? (1 point)



Expliquer le processus de création du JWT et de son utilisation. (2 points)

Le JWT token possède 3 couches dans son encodage. Il a le Header, le Payload et la signature vérifié
voici un exemple concret. Le header contient l'algorithme, le payload contient les informations sur le sujet et le dernier encode les deux premier et créer une signature.

Encoded

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9zIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36P0k6yJV_adQssw5c

Type of token

Decoded

HEADER:

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

PAYLOAD:

```
{
  "sub": "1234567890",
  "name": "John Doe",
  "iat": 1516239022
}
```

VERIFY SIGNATURE

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
  your-256-bit-secret
)
```

☐ secret base64 encoded

Signature Verified

SHARE JWT

Démontrez que l'authentification JWT fonctionne en créant une requête curl pour créer un nouveau post. (2 points)

```
(kali@kali2024blue)~$ curl -X POST -i http://10.0.67.244/wp-json/wp/v2/posts/ -d '{"title":"Jean-Marc"}' -H "Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9zIiwiaWF0IjoxNTE2MjM5MDIyfQ.SflKxwRJSMeKKF2QT4fwpMeJf36P0k6yJV_adQssw5c" -H "Content-Type:application/json"
HTTP/1.1 201 Created
Date: Tue, 06 Feb 2025 14:04:46 GMT
Server: Apache/2.4.58 (Ubuntu)
X-Robots-Tag: noindex
Link: <http://10.0.67.244/wp-json/>; rel="https://api.w.org/" methods
X-Content-Type-Options: nosniff
Access-Control-Expose-Headers: X-WP-Total, X-WP-TotalPages, Link
Access-Control-Allow-Headers: Authorization, X-WP-Nonce, Content-Disposition, Content-MD5, Content-Type
Location: http://10.0.67.244/wp-json/wp/v2/posts/16
Allow: GET, POST
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0, no-store, private
Content-Length: 2535
Content-Type: application/json; charset=UTF-8

{"id":16,"date":"2025-02-04T14:04:46","date_gmt":"2025-02-04T14:04:46","guid":{"rendered":"http://10.0.67.244/?p=16"},"raw":{"http://10.0.67.244/?p=16"},"modified":"2025-02-04T14:04:46","modified_gmt":"2025-02-04T14:04:46","pass_word":"","slug":"","status":"draft","type":"post","link":"http://10.0.67.244/?p=16","title":{"raw":"Jean-Marc","rendered":"Jean-Marc"},"content":{"raw":"","rendered":"","protected":false,"block_version":0},"excerpt":{"raw":"","rendered":"","protected":false},"author":1,"featured_media":0,"comment_status":"open","ping_status":"open","sticky":false,"template":"","format":"standard","meta":{"footnotes":"","categories":[1],"tags":[],"permalink_template":"http://10.0.67.244/2025/02/04/?p=16","generated_slug":"jean-marc","class_list":["post-16","post","type-post"],"status-draft":{"format":"standard","hentry","category-uncategorized"},"links":{"self":{"href":"http://10.0.67.244/wp-json/wp/v2/posts/16"},"targetHints":{"allow":["GET","POST","PUT","PATCH","DELETE"]},"collection":{"href":"http://10.0.67.244/wp-json/wp/v2/posts"},"about":{"href":"http://10.0.67.244/wp-json/wp/v2/types/post"},"author":{"embeddable":true,"href":"http://10.0.67.244/wp-json/wp/v2/users/1"},"replies":{"embeddable":true,"href":"http://10.0.67.244/wp-json/wp/v2/comments?post=16"},"version-history":{"count":0,"href":"http://10.0.67.244/wp-json/wp/v2/posts/16/revisions"},"wp:attachment":{"href":"http://10.0.67.244/wp-json/wp/v2/media?parent=16"},"wp:term":{"taxonomy":"category","embeddable":true,"href":"http://10.0.67.244/wp-json/wp/v2/categories?post=16"},"wp:action-publish":{"href":"http://10.0.67.244/wp-json/wp/v2/posts/16"},"wp:action-unpublish":{"href":"http://10.0.67.244/wp-json/wp/v2/posts/16"},"wp:action-sticky":{"href":"http://10.0.67.244/wp-json/wp/v2/posts/16"},"wp:action-assign-author":{"href":"http://10.0.67.244/wp-json/wp/v2/posts/16"},"wp:action-create-categories":{"href":"http://10.0.67.244/wp-json/wp/v2/posts/16"},"wp:action-assign-categories":{"href":"http://10.0.67.244/wp-json/wp/v2/posts/16"},"wp:action-create-tags":{"href":"http://10.0.67.244/wp-json/wp/v2/posts/16"},"wp:action-assign-tags":{"href":"http://10.0.67.244/wp-json/wp/v2/posts/16"},"curies":{"name":"wp","href":"https://api.w.org/{rel}","templated":true}}}
```


Posts
Add New Post

All (4) | Mine (3) | Published (2) | Drafts (2)
Search Posts

Bulk actions
Apply
All dates
All Categories
Filter
4 items

<input type="checkbox"/> Title	Author	Categories	Tags		Date
<input type="checkbox"/> Jean-Marc — Draft	Ubuntu	Uncategorized	—	—	Last Modified 2025/02/04 at 2:04 pm
<input type="checkbox"/> michel — Draft	Ubuntu	Uncategorized	—	—	Last Modified 2025/02/04 at 1:43 pm
<input type="checkbox"/> Pierre-jean pour vous aider	Jean-Marc Solution	Uncategorized	—	—	Published 2025/01/30 at 5:53 pm
<input type="checkbox"/> piere-jean	Ubuntu	Uncategorized	—	1	Published 2025/01/23 at 5:34 pm
<input type="checkbox"/> Title	Author	Categories	Tags		Date

Bulk actions
Apply
4 items

Fin du laboratoire.